ESET reserachers discover Industroyer, the biggest threat to industrial control systems since Stuxnet

GLOBAL PRESS RELEASE

CATEGORY 1 – GLOBAL

Gothenburg – Sweden, June 13th, 2017

Industroyer is sophisticated and extremely dangerous malware designed to disrupt critical industrial processes.

[ESET](http://www.eset.com/int/) researchers analyzed samples of the malware, detected by ESET as Win32/Industroyer, capable of performing an attack on power supply infrastructure. The malware was most probably involved in the December 2016 attack on Ukraine’s power grid that deprived part of its capital, Kiev, of power for an hour.

*“The recent attack on the Ukrainian power grid should serve as a wake-up call for all those responsible for the security of critical systems around the world,”* warns Anton Cherepanov, ESET Senior Malware Researcher.

ESET researchers discovered Industroyer is capable of directly controlling electricity substation switches and circuit breakers. It uses industrial communication protocols used worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure. The potential impact may range from simply turning off power distribution through triggering a cascade of failures, to more serious damage to equipment.

 

*Scheme of Industroyer operation*

*“Industroyer’s ability to persist in the system and to directly interfere with the operation of industrial hardware makes it the most dangerous malware threat to industrial control systems since the infamous Stuxnet, which successfully attacked Iran’s nuclear program and was discovered in 2010,”* concludes Anton Cherepanov.

Additional technical details on the malware, including Indicators of Compromise, can be found in an [article](https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/) and in a comprehensive [white paper](https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf) at ESET’s blog, [WeLiveSecurity.com](https://www.welivesecurity.com/).

About ESET

For 30 years, [ESET®](http://www.eset.com/int/) has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET’s high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn [100 Virus Bulletin VB100](https://www.eset.com/int/about/newsroom/awards/eset-first-to-break-magical-100-vb100-awards-threshold/) awards, identifying every single “in-the-wild” malware without interruption since 2003. For more information visit [www.eset.com](http://www.eset.com/about) or follow us on [LinkedIn](https://www.linkedin.com/company/28967?trk=tyah&trkInfo=tarId%3A1402921556545%2Ctas%3AESET%2Cidx%3A2-1-4), [Facebook](https://www.facebook.com/eset?ref=br_tf) and [Twitter](https://twitter.com/ESET).